In Douglas, a host-based IDS sensor (or "HIDS sensor") 20 detects attacks targeted at a host system "on which it is installed, e.g., on a web server 1, a domain name server (DNS server) 2, a mail server 3, etc." (see column 2, lines 30-34). As described in column 2, lines 38-41, the HIDS sensor 20 monitors logs of applications running on the host such as mail servers 3, web servers 1, and FTP servers.

In Douglas, the HIDS sensor 20 is installed on a host system, and various applications (e.g., mail servers, web servers, etc.) also run on the host system, and thus the HIDS sensor and the applications together make up the same system. Therefore, the HIDS sensor 20 of Douglas is **not** arranged separately from an intrusion detection system.

Moreover, the HIDS sensor 20 of Douglas does not collect, store, and manage logs of an intrusion detection system as claimed.

In particular, the HIDS sensor 20 of Douglas does not collect a log of a **separate** intrusion detection system. Instead, the HIDS sensor 20 is part of the IDS itself, and directly monitors attacks on the host system (see, e.g., column 2, lines 30-34, as described above).

Further, in the Office Action of 04/03/2008, the Examiner did not respond to the following arguments included in the Amendment filed on January 16, 2008:

> Further, there is simply no teaching or suggestion in Douglas of the claimed analysis of statistics of logs managed by a database. In Douglas, the monitoring of system output and audit logs performed within the IDS is not equivalent to the claimed "log analysis section" that obtains statistics and performs statistical analysis based on logs stored in a database.
>
> The Maier reference was cited allegedly for teaching a database (see page 4 of Office Action of 10/01/2007).

In Maier, a database is disclosed in which the structure of a database table or index can be altered "while the database table or index remains available for execution of transactions" (see column 2, lines 39-43 of Maier).

However, Maier does not teach or suggest a database that "stores and manages logs collected by the log collection section" (independent claim 1; *see also* independent claims 11 and 21).

Moreover, Maier is not related to a log analysis support apparatus, method, or program, and is not even directed to an intrusion detection system. In Maier, the database is structured to allow continued availability for transaction execution even while the database is being altered, which is not relevant to the Applicants' claimed invention in which a database must store and manage logs collected by a log collection section.

Therefore, the proposed combination of Douglas in view of Maier does not teach or suggest the Applicants' claimed IDS log analysis support apparatus, method or program.

It is believed the application is in condition for immediate allowance, which action is earnestly solicited.

Respectfully submitted,

/Steven M. Jensen/

Date: August 1, 2008

Steven M. Jensen
(Reg. No. 42,693)
Edwards Angell Palmer & Dodge
P.O. Box 55874
Boston, MA 02205

Phone: (617) 239-0100

Customer No. 21874